

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

USDC SDNY DOCUMENT ELECTRONICALLY FILED DOC #: DATE FILED: 4/15/2020
--

-----X
HELENE DEUTSCH,

Plaintiff,

-against-

HUMAN RESOURCE MANAGEMENT, INC.,
THE HRM CAPSTONE PARTNERSHIP, INC.
(D/B/A THE CAPSTONE PARTNERSHIP),
ADP TOTALSOURCE CO. XXI INC., and
ROLFE I. KOPELAN,

Defendants.

-----X

19-CV-5305 (VEC)

OPINION AND ORDER

VALERIE CAPRONI, United States District Judge:

Plaintiff Helene Deutsch alleges violations of the Computer Fraud and Abuse Act (“CFAA”) and asserts various state law claims against Defendants Human Resource Management, Inc. (“HRM”), The HRM Capstone Partnership, Inc. (“Capstone”), ADP Totalsource Co. XXI Inc. (“ADP”), and Rolfe I. Kopelan (“Kopelan”) (collectively, “Defendants”). Am. Compl. (Dkt. 22). The Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1367. HRM, Capstone, and Kopelan (collectively, “Capstone Defendants”) have moved to dismiss the Amended Complaint under Federal Rule of Civil Procedure 12(b)(6) and 12(b)(1).¹ Mot. (Dkt. 31). Because the Court finds that Plaintiff failed

¹ Although the Capstone Defendants style their pleadings as a Rule 12(b)(6) motion, because they also argue that the Court should decline to exercise supplemental jurisdiction over the state law claims, the Court will construe their motion as having been made under Rule 12(b)(1) as well.

to state a claim for relief under CFAA and the Court declines to exercise supplemental jurisdiction over Plaintiff's state law claims, the motion to dismiss is GRANTED.²

BACKGROUND³

Capstone is an executive recruiting firm and a wholly-owned subsidiary of HRM. Am. Compl. ¶¶ 7, 23, 29. Kopelan is the controlling shareholder of HRM and the managing partner of Capstone. *Id.* ¶ 24. Around November 2008, Plaintiff became a partner at Capstone, working as an executive recruiter for senior-level legal positions. *Id.* ¶¶ 30–31. Plaintiff was entitled to an annual draw, payable semi-monthly, and commissions, payable monthly. *Id.* ¶¶ 32, 34.

By February 2019, relations among the partners had deteriorated. Plaintiff received neither her semi-monthly draw nor her commissions. *Id.* ¶ 39. Plaintiff was told that Capstone would be forced to “close shop” in a week unless she agreed to reduce her commissions and eliminate her salary. *Id.* ¶¶ 41–44, 46. In March, Kopelan's attorney offered to pay Plaintiff the compensation she was owed if she would resign from Capstone. *Id.* ¶¶ 51–52. Plaintiff declined to voluntarily resign, eliminate her salary, or reduce her commissions. *Id.* ¶ 53. On March 15 Plaintiff was paid her previously owed commission, but she still did not receive her semi-monthly draw. *Id.* ¶ 55.

On March 22, 2019, Kopelan represented to Plaintiff's attorney that Capstone would cease operations a week later. *Id.* ¶¶ 57–59. Faced with the closing of Capstone, Plaintiff accepted employment with a third party. *Id.* ¶ 61. But when Plaintiff went to Capstone's offices

² ADP has also moved to dismiss the Amended Complaint pursuant to Rule 12(b)(6). Mot. (Dkt. 24). Because granting the Capstone Defendants' motion to dismiss results in dismissal of the entire case, the Court need not address ADP's separate motion.

³ The facts are based on the allegations contained in the Amended Complaint. The Court accepts all well-pled, non-conclusory factual allegations in the pleadings as true and draws all reasonable inferences in the light most favorable to Plaintiff. *See Gibbons v. Malone*, 703 F.3d 595, 599 (2d Cir. 2013).

to retrieve her personal belongings, she saw that all the offices and cubicles were intact except for the office of an employee who had worked exclusively with Plaintiff and the cubicle of an employee who had an EEOC charge of sexual harassment pending against Capstone. *Id.* ¶¶ 62–65. According to Plaintiff, the announced closure of Capstone was merely a scheme by Kopelan and Capstone to terminate her employment. *Id.* ¶ 67.

On April 4, 2019, Plaintiff’s personal telephone, which she also used to access Capstone email and applications, was “wiped” and restored to factory settings. *Id.* ¶¶ 73, 76–77. In addition to work data, Plaintiff lost “irreplaceable photographs, personal and professional contacts, text messages, passwords, and personal software applications.” *Id.* ¶ 75. Plaintiff had been required to use her telephone for work because Defendants did not issue one. *Id.* ¶ 73. Defendants did not have a policy that permitted them to wipe personal content from employees’ telephones remotely, nor did they ever ask for Plaintiff’s consent to access or “wipe” her phone. *Id.* ¶ 74. Other former employees, by contrast, had only their Capstone email accounts remotely wiped. *Id.* ¶ 81. Plaintiff alleges that Kopelan authorized Capstone to remotely wipe Plaintiff’s telephone in retaliation for her demands for compensation and her complaint to ADP,⁴ which ultimately terminated its contract with Capstone. *Id.* ¶ 80.

DISCUSSION

I. Standard of Review

To survive a motion to dismiss under Rule 12(b)(6), “a complaint must allege sufficient facts, taken as true, to state a plausible claim for relief.” *Johnson v. Priceline.com, Inc.*, 711 F.3d 271, 275 (2d Cir. 2013) (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555–56 (2007)). “[A]

⁴ In early March, Plaintiff had called ADP—a third-party human resources service provider for Capstone employees—and complained about her unpaid compensation and alleged misconduct by Kopelan. *Id.* ¶ 49.

complaint does not need to contain detailed or elaborate factual allegations, but only allegations sufficient to raise an entitlement to relief above the speculative level.” *Keiler v. Harlequin Enters., Ltd.*, 751 F.3d 64, 70 (2d Cir. 2014) (citation omitted). The court is not required, however, to credit “mere conclusory statements” or “threadbare recitals of the elements of a cause of action.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Twombly*, 550 U.S. 544, 555 (2007)). Courts are generally confined to “the four corners of the complaint” and must “look only to the allegations contained therein.” *Perez v. Westchester Foreign Autos, Inc.*, No. 11-CV-6091, 2013 WL 749497, at *5 (S.D.N.Y. Feb. 28, 2013) (citing *Roth v. Jennings*, 489 F.3d 499, 509 (2d Cir. 2007)).

II. Plaintiff Fails to State a Claim Under the CFAA

Plaintiff’s first claim arises under the CFAA and is alleged only against Kopelan and Capstone. *See* Am. Compl. ¶¶ 82–87. The CFAA is principally a criminal statute that prohibits “[f]raud and related activity in connection with computers,” 18 U.S.C. § 1030, but it also provides a private right of action to “[a]ny person who suffers damage or loss by reason of a violation of this section,” *id.* § 1030(g).⁵ “[T]he scope of the civil actions permitted under . . . Section 1030(g), however, has always been limited.” *Hancock v. Cty. of Rensselaer*, 882 F.3d 58, 63 (2d Cir. 2018). To maintain her action, Plaintiff must allege that Defendants “intentionally accesse[d] a protected computer without authorization, and as a result of such conduct, cause[d] damage and loss.” 18 U.S.C. § 1030(a)(5)(C). Plaintiff must also allege “economic damages” “aggregating at least \$5,000 in value.” *Id.* §§ 1030(c)(4)(A)(i)(I), (g). Plaintiff has failed to allege either element.

⁵ There is no dispute that Plaintiff’s telephone is a protected device under the statute.

A. Plaintiff Fails to Allege that Kopelan and Capstone Accessed Her Telephone “Without Authorization”

The Amended Complaint asserts that Kopelan and Capstone acted “without authorization” when they erased personal data stored on her telephone on April 4, 2019. Am. Compl. ¶ 84. Plaintiff argues that because she had not given them permission to do so, they acted “without authorization” under the CFAA (notwithstanding that she acknowledges in the Amended Complaint that the telephone was also used for work purposes and implicitly acknowledges that Kopelan and Capstone had authorization to delete work data). Pl.’s Opp. (Dkt. 36) 6–8; *see* Am. Compl. ¶¶ 73, 81.

The law is clear in the Second Circuit that the CFAA imposes liability only on persons who gain access to a protected system when that access was not authorized.⁶ *United States v. Valle*, 807 F.3d 508, 511–12 (2d Cir. 2015). In *Valle*, the defendant used his authorized access to restricted databases for personal purposes in contravention of work policy.⁷ *Id.* at 512–13. He was convicted of violating a CFAA provision that criminalizes accessing a protected device “without authorization or exceed[ing] authorized access.” *Id.* at 512–13; 18 U.S.C. § 1030(a)(2)(B). Because the *Valle* defendant was not wholly “without authorization” to access the databases at issue, the dispositive question on appeal was whether he “exceeded [his]

⁶ There is a split of authority at the Circuit level on this issue. In addition to the Second Circuit, the Fourth and Ninth Circuits subscribe to the narrow approach articulated in the main text. *See WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012); *United States v. Nosal*, 676 F.3d 854, 862–63 (9th Cir. 2012) (en banc). The First, Fifth, Seventh, and Eleventh Circuits, in contrast, have adopted a “broad” approach, extending liability to persons who misuse information on a protected device to which they had legitimate access. *See United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010); *United States v. John*, 597 F.3d 263, 271 (5th Cir. 2010); *Int’l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420–21 (7th Cir. 2006); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581–84 (1st Cir. 2001).

⁷ Although *Valle* was a criminal case involving a different subsection of CFAA, its holding applies to civil cases. The Supreme Court has determined that courts, when analyzing a statute that “has both criminal and noncriminal applications . . . must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context” *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004).

authorized access.” *Id.* at 523. The Second Circuit reversed the conviction, holding that a person who has permission to access a computer system and later uses that access for an improper purpose has not “exceed[ed] [his] authorized access.” *Id.* at 527–28. In reaching its decision, the Second Circuit noted that “‘without authorization’ most naturally refers to a scenario *where a user lacks permission to access the computer at all.*” *Id.* at 524 (emphasis added); *see also JBCHoldings NY, LLC v. Pakter*, 931 F. Supp. 2d 514, 523 (S.D.N.Y. 2013) (“The common meaning of ‘without authorization’ is ‘without any permission at all.’”).⁸

Following *Valle*, district courts have consistently looked to whether the person had authorized access to the device. *See, e.g., Fischkoff v. Iovance Biotherapeutics, Inc.*, 339 F. Supp. 3d 408, 419 (S.D.N.Y. 2018) (holding that there was no CAFA claim based on allegations that the party “accessed materials that his credentials permitted him to access but that the Employee Handbook instructed him not to access”); *Associated Mortg. Bankers, Inc. v. Calcon Mut. Mortg. LLC*, 159 F. Supp. 3d 324, 334–35 (E.D.N.Y. 2016) (holding that the defendants’ “alleged misappropriation of [the plaintiff’s] loans” did not plead that the defendant entered one of plaintiff’s computers “without authorization” or in “excess of authorization”). That focus is consistent with the statute’s purpose: to combat “hacking, i.e., trespass into computer systems or data.” *Valle*, 807 F.3d at 526; *see also United States v. Nosal*, 676 F.3d 854, 858 (9th Cir. 2012) (en banc) (“‘Without authorization’ would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and ‘exceeds authorized access’ would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files).”). The Ninth Circuit has recently reaffirmed these principles,

⁸ This case is a good illustration of the Second Circuit’s concern that the broader approach adopted by some other circuits risks criminalizing “the conduct of millions of ordinary computer users and plac[ing] [the Court] in the position of a legislature.” *Valle*, 807 F.3d at 527.

holding that “the CFAA’s prohibition on accessing a computer ‘without authorization’ is violated when a person circumvents a computer’s generally applicable rules regarding access permissions, such as username and password requirements.” *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1003 (9th Cir. 2019).

Plaintiff makes clear that when she says Kopelan and Capstone accessed her telephone “without authorization,” she means that they abused their access by deleting personal data that resided on her telephone. This is fatal to Plaintiff’s case. Plaintiff asserts that Kopelan and Capstone violated the CFAA when they deleted her personal data, Am. Compl. ¶¶ 78–80; she does not allege that they had no authorization to access the telephone at all, or even that parts of her phone were walled off to Kopelan and Capstone. Nor does Plaintiff allege how Kopelan and Capstone accessed her telephone, such as by circumventing a firewall or otherwise hacking through technological barriers. *See, e.g., LivePerson, Inc. v. 24/7 Customer, Inc.*, 83 F. Supp. 3d 501, 513 (S.D.N.Y. 2015) (finding a plaintiff’s CFAA allegations failed to “discuss the means by which the [d]efendants allegedly gained access to [the] systems and so [could not] be construed as establishing that the [d]efendant either lacked or exceeded its authorization within the meaning of the CFAA.”). Rather, the Amended Complaint includes several allegations that appear to acknowledge that Kopelan and Capstone had permission to access her device. For example, she alleges that they did not give her “notice” regarding the wiping of her telephone, Am. Compl. ¶ 85, that “Kopelan authorized Capstone to wipe Plaintiff’s Phone by remote,” *id.* ¶ 80, that Defendants “required her to use her own smartphone . . . to access work email and applications,” *id.* ¶ 73, and that “at all prior times that other employees have terminated their

employment relationships with Defendants, Kopelan and Capstone only remotely deleted the Capstone email account from the former employees' phones," *id.* ¶ 81.⁹

Widening this unbridgeable gap, Plaintiff also alleges that Kopelan and Capstone "did not have in place any policy permitting them to wipe content from the Phone remotely." *Id.* ¶ 74. But just as CFAA does not apply to "an employee who has been granted access to an employer's computer and misuses that access, either by violating the terms of use or by breaching a duty of loyalty," *Chefs Diet Acquisition Corp. v. Lean Chefs, LLC*, No. 14-CV-8467, 2016 WL 5416498, at *6 (S.D.N.Y. Sept. 28, 2016)), the fact that an employer does not have a policy or agreement sanctioning a particular activity does not give rise to a CFAA violation if the employer had authority to access the device where the purported misuse occurred.

B. Plaintiff Also Fails to Allege Compensable Losses of \$5,000

Plaintiff also has not adequately alleged the type and amount of losses necessary to state a CFAA claim. Losses are compensable under the CFAA only when caused by damage to or impairment of the protected device. *Civic Ctr. Motors, Ltd. v. Mason St. Imp. Cars, Ltd.*, 387 F. Supp. 2d 378, 381 (S.D.N.Y. 2005) (citing *Nexans Wires S.A. v. Stark-USA, Inc.*, 319 F. Supp. 2d 468, 474 (S.D.N.Y. 2004), *aff'd*, 166 Fed. App'x 559 (2d Cir. 2006)). Alleged losses must also meet the minimum \$5,000 threshold. 18 U.S.C. § 1030(c)(4)(A)(i)(I).

⁹ In her opposition brief, Plaintiff argues that any authorization the Capstone Defendants had to access her telephone should have halted when her employment ended. Pl.'s Opp. at 7. In the reverse scenario—an employee's access to an employer's computer system—courts have found that "access will be construed as unauthorized within the meaning of the CFAA only where it occurs after the employee is terminated or resigns." *Poller v. BioScrip, Inc.*, 974 F. Supp. 2d 204, 233 (S.D.N.Y. 2013). But Plaintiff has not explained why an employer, much less her own employer, would automatically lose authorization to access an employee's work-related device (even if that device is personally owned as a matter of property law) when employment comes to an end. In any event, Plaintiff does not allege that her employment had ended prior to this incident; to the contrary, she alleges that she requested her draw and commissions through April 15, 2019, suggesting that her employment had not terminated when the Capstone Defendants accessed her telephone on April 4. Am. Compl. ¶¶ 71, 76; see *In re Agape Litig.*, 773 F. Supp. 2d 298, 316 (E.D.N.Y. 2011) ("It is well-settled that a plaintiff cannot amend the complaint through briefs and affidavits, and such facts are thus irrelevant for purposes of determining whether the [p]laintiff's complaint should be dismissed for failure to state a claim." (quotation omitted)).

This Court agrees with the majority of decisions in this Circuit finding that “loss” means the “cost of investigating or remedying damage to a computer, or a cost incurred because the computer’s service was interrupted.” *Nexans*, 319 F. Supp. 2d at 475. That includes “any remedial costs of investigating the computer for damage, remedying the damage and any costs incurred because the computer cannot function while or until repairs are made.” *Garland-Sash v. Lewis*, No. 05-CV-6827, 2011 WL 6188712, at *4 (S.D.N.Y. Dec. 6, 2011) (quoting *Nexans*, 319 F. Supp. 2d at 474). Compensable losses do not include, for example, “damages for death, personal injury, mental distress, and the like.” *Bose v. Interclick, Inc.*, No. 10-CV-9183, 2011 WL 4343517, at *4 (S.D.N.Y. Aug. 17, 2011) (quoting *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 935 (9th Cir. 2004)).

Plaintiff’s losses are not the type of losses contemplated by the CFAA. Plaintiff’s claim is based on the loss of personal data from her telephone, including “irreplaceable photographs, personal and professional contacts, text messages, passwords, and personal software applications.” Am. Compl. ¶ 75. There is no allegation that losses were incurred from efforts to identify, diagnose, or address damage to the protected device or from an interruption of service. *See, e.g., In re Doubleclick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 524–25 (S.D.N.Y. 2001) (rejecting plaintiff’s claim for the economic value of lost consumer attention); *Nexans*, 319 F. Supp. 2d at 478 (rejecting plaintiff’s claim for lost revenues and the costs of business trips taken in response to a computer hacking incident); *Univ. Sports Pub. Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 388 (S.D.N.Y. 2010) (rejecting as compensable damages costs incurred shoring up the security of a database, even if prompted by the initial hacking). Plaintiff has not alleged, for example, that she incurred costs restoring the data that was on her telephone, investigating the intrusion, or restoring service.

Plaintiff has also failed to allege facts from which the Court could infer that she has met the minimum loss threshold for a civil claim under the CFAA. “[A]ny civil action under the CFAA involving ‘damage or loss’ must satisfy the \$ 5,000 threshold.” *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 439 (2d Cir. 2004). Plaintiff alleges that the “permanent loss and destruction” of her property “caused loss in excess of \$5,000,” Am. Compl. ¶¶ 85–86, but she has not alleged what costs she incurred. Those conclusory allegations are insufficient. *See, e.g., Law Firm of Omar T. Mohammedi, LLC v. Computer Assisted Practice Elec. Mgmt. Sols.*, No. 17-CV-4567, 2019 WL 3288390, at *7 (S.D.N.Y. July 22, 2019) (noting that “courts within this District have dismissed CFAA claims for failing to sufficiently quantify damages” and collecting cases). Because Plaintiff alleges only that she incurred more than \$5,000 in damages, she has not adequately alleged that she satisfied the CFAA threshold.

III. Amendment of the Complaint Would Be Futile

As a general rule, a “court should freely give leave” to amend a complaint “when justice so requires.” Fed. R. Civ. P. 15(a)(2). “Notwithstanding the liberality of the general rule, [w]hether to allow amendment is a decision that rests in the discretion of the district court.” *Lincoln v. Potter*, 418 F. Supp. 2d 443, 454 (S.D.N.Y. 2006) (quotation omitted). Leave to amend may be denied for good reason, including where amendment would be futile. *Schiro v. Cemex, S.A.B. de C.V.*, 396 F. Supp. 3d 283, 308 (S.D.N.Y. 2019). “[W]here the problems with a claim are ‘substantive’ rather than the result of an ‘inadequately or inartfully pleaded’ complaint, an opportunity to replead would be ‘futile’ and ‘should be denied.’” *Lopez v. Ctpartners Exec. Search Inc.*, 173 F. Supp. 3d 12, 44 (S.D.N.Y. 2016) (quoting *Cuoco v. Moritsugu*, 222 F.3d 99, 112 (2d Cir. 2000)).

In this case, Plaintiff has already amended her complaint once. Giving her leave to amend again would be futile. It is clear that Plaintiff's CFAA claim is about Kopelan and Capstone allegedly misusing the access they had to her telephone—not that they lacked authority to access the device in the first place. She therefore cannot state a claim that they acted “without authorization” under the CFAA. 18 U.S.C. § 1030(a)(5). Although her allegations might more plausibly present an “exceeds authorized access” case, there is no hint that Kopelan and Capstone hacked Plaintiff's phone from the “inside,” *i.e.*, circumvented barriers to gain access to parts of Plaintiff's telephone from which they had been excluded.¹⁰ As a result, no amendment would salvage her CFAA claim. Moreover, Plaintiff's alleged losses are categorically non-compensable under the CFAA. That is yet another hurdle that Plaintiff cannot overcome.

IV. The Court Declines to Exercise Supplemental Jurisdiction

As to Plaintiff's remaining state law claims, “district courts may decline to exercise supplemental jurisdiction over a claim” where the court “has dismissed all claims over which it has original jurisdiction.” 28 U.S.C. § 1367(c)(3). Although Section 1367(c) is “permissive rather than mandatory, . . . where all the federal claims have been dismissed at a relatively early stage, the district court should decline to exercise supplemental jurisdiction over pendent state-law claims.” *Astra Media Grp., LLC v. Clear Channel Taxi Media, LLC*, 414 F. App'x 334, 337 (2d Cir. 2011). Because Plaintiff has failed to state a federal cause of action under the CFAA, and minimal effort has thus far been invested in this litigation, the Court will not retain jurisdiction over Plaintiff's remaining state law claims.

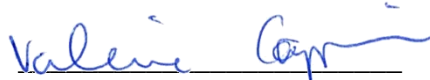
¹⁰ Moreover, the Court notes that Section 1030(a)(5) does not circumscribe access that “exceeds authorized access”; it prohibits only access “without authorization.” Consequently, Plaintiff would not be able to pursue a Section 1030(a)(5) violation. Plaintiff would instead have to allege violations of Sections 1030(a)(1), (2), (4), or (7), which are even less well-fitted to her allegations.

CONCLUSION

For the foregoing reasons, the Capstone Defendants' motion to dismiss the Amended Complaint is GRANTED. Plaintiff's CFAA claim is dismissed with prejudice, without leave to amend, and Plaintiff's state law claims are dismissed without prejudice. The Clerk of Court is respectfully directed to terminate all open motions and close this case.

SO ORDERED.

Date: April 15, 2020
New York, New York


VALERIE CAPRONI
United States District Judge